#2

1503.65307 PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application)
)
Applicant: Takayoshi Kurita)
)
Serial No.)
)
Filed: March 14, 2001)
)
For: SMART CARD ACCESS)
MANAGEMENT SYSTEM,)
SHARING METHOD, AND)
STORAGE MEDIUM)
)
Art Unit:)

I hereby certify that this paper is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on March 14, 2001.
Express Label No.: EL 846162085 US
Signature: L. Davila

CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

Applicant claims foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 2000-269096, filed September 5, 2000.

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By

Patrick G. Burns
Reg. No. 29,367

March 14, 2001
300 South Wacker Drive
Suite 2500
Chicago, IL 60606
(312) 360-0080
Customer Number: **24978**

#2

PATANT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: September 5, 2000

Application Number: Patent Application
No. 2000-269096

Applicant(s): FUJITSU LIMITED

December 1, 2000

Commissioner,
Patent Office Kozo OIKAWA

Certificate No. 2000-3098184

1503.65307
(312) 360-0080
#2

J1017 U.S. PTO
09/809736
03/14/01

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年　９月　５日

出 願 番 号
Application Number: 特願２０００－２６９０９６

出 願 人
Applicant (s): 富士通株式会社

２０００年１２月　１日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号　出証特２０００－３０９８１８４

【書類名】　特許願

【整理番号】　0051322

【提出日】　平成12年 9月 5日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/00

【発明の名称】　スマートカードのアクセス管理システム、共有方法及び記憶媒体

【請求項の数】　10

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　栗田　享佳

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100074099

【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ

【弁理士】

【氏名又は名称】　大菅　義之

【電話番号】　03-3238-0031

【選任した代理人】

【識別番号】　100067987

【住所又は居所】　神奈川県横浜市鶴見区北寺尾７－２５－２８－５０３

【弁理士】

【氏名又は名称】　久木元　彰

【電話番号】　045-573-3683

【手数料の表示】

【予納台帳番号】　012542

【納付金額】　　21,000円

【提出物件の目録】

【物件名】　　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9705047

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　スマートカードのアクセス管理システム、共有方法及び記憶媒体

【特許請求の範囲】

【請求項１】　複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードのアクセス管理システムであって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする排他制御手段と、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可するアクセス制御手段と

を備えることを特徴とするアクセス管理システム。

【請求項２】　前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録することを特徴とする請求項１に記載のアクセス管理システム。

【請求項３】　前記アクセス制御手段は、前記アクセス要求に対し、前記排他を獲得したアプリケーションが前記スマートカードから未認証である時、該アプリケーションの要求を拒否することを特徴とする請求項１又は２に記載のアクセス管理システム。

【請求項４】　前記アクセス制御手段は、前記スマートカードがスマートカードリーダより抜かれた時、該抜かれたスマートカードにより認証済みとなっているアプリケーションを未認証に変更することを特徴とする請求項１乃至３のいずれか１に記載のアクセス管理システム。

【請求項５】　前記アプリケーションは、前記スマートカードに複数回アクセ

スする時、各アクセスの開始時に前記排他制御手段に前記排他獲得要求を行い、該各アクセスの終了時に前記排他制御手段に排他の解除通知を行うことを特徴とする請求項１乃至４のいずれか１に記載のアクセス管理システム。

【請求項６】　前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードが他のアプリケーションによって既に排他獲得済みであれば、該排他獲得要求を行ったアプリケーションをキューに登録し、前記アプリケーションからの排他の解除通知に対し、前記キューに登録されているアプリケーションを排他獲得済みとすることを特徴とする請求項５に記載のアクセス管理システム。

【請求項７】　前記アクセス制御手段は、アプリケーションからスマートカードの認証解除の通知に対し、該認証解除が該スマートカードにより認証済みとなっている最後のアプリケーションからの時、該スマートカードに認証解除を要求することを特徴とする請求項１乃至６のいずれか１に記載のアクセス管理システム。

【請求項８】　複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードの共有方法であって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを特徴とする共有方法。

【請求項９】　１つのスマートカードへの複数のアクセス処理を含むアプリケーション又はそのライブラリであって、

前記各アクセス処理に対し、該アクセス処理の開始時にそれぞれ前記排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、

前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーション又はそ

のライブラリ。

【請求項１０】　複数のアプリケーションが並列動作する情報処理装置によって使用された時、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを前記情報処理装置に行わせるプログラムを記憶した前記情報処理装置が読み出し可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、スマートカード上のデータの複数プロセスによる共有した場合のスマートカードのアクセス管理に関する。

【０００２】

【従来の技術】

スマートカードは、従来用いられている磁気カードに比して非常に大きな容量のデータを記憶することが出来ることなどから、様々な分野への使用が検討され、あるいは実用化されている。

【０００３】

またスマートカードは、内部にメモリ共にＣＰＵを備えており、このＣＰＵを介してメモリ内のデータへアクセスを行うので、アクセス時にＣＰＵに認証処理を行わせることにより、従来の磁気カードに比べて高いセキュリティ性を実現出来、この点もスマートカードのメリットとなっている。

【０００４】

スマートカードはＰＩＮ（Personal Identification Number）によるセキュリティ機能を持っており、この機能によりＰＩＮの照合を行い、認証された場合に

だけカード内の秘密情報をアクセスすることができるように制御することが可能である。このＰＩＮによる認証は、いわゆるパスワード入力方式で、スマートカードを用いるユーザがＰＩＮとして例えばパスワードを入力し、これをスマートカード内に記憶しているパスワードとカード内で比較して、一致した場合に内部データへのアクセスを許可する。

【０００５】

スマートカードへのアクセスは、スマートカードが持つ論理チャネルを通して行い、認証要求は論理チャネルに対して行われる。そしてスマートカードは、この論理チャネル毎にＰＩＮによる認証状態などセキュリティに関する状態を保持している。

【０００６】

図１５は、アプリケーションから見たスマートカード内部の論理的構成を示したものである。

スマートカード内では、データをツリー構造の構成によって管理しており、最上位にあるＤＩＲの下層に、使用されるアプリケーション毎の単位等でＤＦ（Delicated File）が設けられている。そして、各ＤＦ内には実際のデータを保持しているＥＦ（Elementary File ）が格納されている。スマートカードからデータを読み出す際、アプリケーションは、まずアクセスを行うデータの位置を示す位置付け情報を送って、目的のＥＦにアクセス位置を移動した後、そのＥＦからデータの読みだし／書込みを行う。また各チャネルは、現在のアクセス位置を状態情報として保持している。

【０００７】

【発明が解決しようとする課題】

現在スマートカードを複数のアプリケーションで同時に使用する使い方が検討されている。例えば公開鍵暗号方式をベースとしたＰＫＩ（Public Key Instructure）システムを構築し、このシステム上のコンピュータで複数のアプリケーションが稼動している場合に、各アプリケーションがデジタル署名などによるセキュリティ認証にスマートカードを用いることが、現在スマートカードの１つの使用方法として考えられている。

【０００８】

この場合、スマートカードを接続したコンピュータ上の複数のアプリケーションがスマートカードを共用することになる。そして多数のアプリケーションに同一のカードに対してアクセスさせる場合、１つのスマートカードが持つ論理チャネルの数はせいぜい２チャネル程度なので、１つの論理チャネルを複数のアプリケーションが共有する必要が出てくる。尚本明細書内の以下の説明は、説明の簡略化のため、１つのアプリケーションは１つのプロセスで構成されることを前提としており、アプリケーションという言葉をプロセスと同義で用いている。通常１つのアプリケーションは１つのプロセスで構成されることが多いが、複数のプロセスで構成されている場合でも、アプリケーションをプロセスと置換えて考えれば、以下の説明は基本的に同じである。

【０００９】

現行のスマートカードのセキュリティ方式では、１つのアプリケーションがある論理チャネルに対してＰＩＮ認証を行いアクセス許可を得ると、以降その論理チャネルからは、認証が解除されるまでの間、認証を受けたアプリケーションだけでなく他のアプリケーションもアクセス出来てしまう。

【００１０】

複数のアプリケーションで１つのカードの同じ情報を共有することを、セキュリティの観点から考えると、個々のアプリケーション毎にＰＩＮによる認証を行った方がセキュリティレベルはより強固になる。しかし、現行のスマートカードへのアクセス制御では、１つの論理チャネルを複数のアプリケーションで共有する場合、論理チャネル毎に認証が行われ各論理チャネルに認証状態（アクセス許可を与えたか否か）が保持されるため、１つのアプリケーションがＰＩＮによる認証を行ってアクセス許可を得れば、他のアプリケーションはＰＩＮによる認証を受けずに、その論理チャネルからカードへのアクセスが可能となってしまう。

【００１１】

また、各上述したように各アプリケーションは、カード内のデータにアクセスする際、位置付け情報を論理チャネルに送信してアクセス位置を移動してからデータの書込み／読みだしを行うが、複数のアプリケーションが論理チャネルを共

有する場合、各アプリケーションはカレントのアクセス位置の把握が難しくなる。

【００１２】

上記問題点を鑑み、本発明は、複数のアプリケーション（プロセス）によるアクセスに対し、スマートカードへの認証状態を一元管理することにより、各アプリケーション（プロセス）毎に認証許可を与えるスマートカードのアクセス管理システム及び管理方法を提供することを課題とする。また、各アプリケーション（プロセス）毎の認証を認証処理によるオーバヘッドを大きくすること無く実現するアクセス管理システム及び管理方法を提供することを課題とする。

【００１３】

【課題を解決するための手段】

上記問題点を解決するため、本発明によるスマートカードのアクセス管理システムは、複数のアプリケーションによるスマートカードへのアクセスを管理するものであって、排他制御手段及びアクセス制御手段を備える。

【００１４】

排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする。また上記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録する。

【００１５】

アクセス制御手段は、排他獲得済みとなっているアプリケーションからの上記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可する。またアクセス制御手段は、上記アクセス要求に対し、上記排他を獲得したアプリケーションが上記スマートカードから未認証である時、該アプリケーションにＰＩＮの入

力を要求する。各アプリケーションによるスマートカードの認証はこのアクセス制御手段を通して行われ、アクセス制御手段は各アプリケーションとスマートカードとの認証関係を把握している。

【００１６】

本発明によれば、排他制御手段により、スマートカードに対する排他制御が行われるので、複数のアプリケーションによってスマートカードを共用しても各アプリケーション毎の認証を可能とする。

【００１７】

また、アクセス制御手段により、各アクセス要求を行ったアプリケーションが認証済みかどうかが判断され、認証済みの場合、認証処理を行わずにアクセス許可を与えるので、認証処理回数を削減することが出来る。

【００１８】

【発明の実施の形態】

以下に本発明の一実施形態について、図面を参照しながら説明する。

各アプリケーション毎に認証許可を与えるようにするためには、スマートカード（スマートカードが複数の論理チャネルをもつ場合論理チャネル）に対して排他制御を行い、認証された１つのアプリケーションがスマートカードを使用している間、そのアプリケーションがカード（若しくは論理チャネル）を専有し、他のアプリケーションからのアクセスを抑止する必要がある。尚説明簡略化の為、以下の実施形態では各スマートカードは論理チャネルを１つ備える構成とする。尚スマートカードが複数論理チャネルを備えた場合は、以下に説明する排他制御は論理チャネル単位で行われる。

【００１９】

図１は、排他制御機構を設け、スマートカードにアクセスするアプリケーションの排他処理を行った場合を示す。

図１では、複数のアプリケーション２１とスマートカード２２の間に排他制御機構１１を設け、スマートカード２２に対してアクセスを要求する際、各アプリケーション２１はこの排他制御機構１１に対して排他獲得要求を行い、排他が得られたアプリケーション２１が、スマートカード２２を専有してアクセスを行う

。同図の排他制御機構１１はカードａ、ｂの２つのカードへのアクセスに対する排他を管理している。そしてアプリ１、アプリ２及びアプリ３の３つのアプリケーション２１がカードａに対してアクセス要求を発行しており、排他制御機構１１はそのうちのアプリ１に対して排他獲得とし、他のアプリ２及び３はカードａが解放されるまで待ち状態にしておく。排他を獲得したアプリ１は、カードａの論理チャネルに対してＰＩＮ認証を行った後データの読みだし／書込みを行う。この間他のアプリケーション２１は、カードａに対してアクセスすることが出来ない。アプリ１が処理を完了してカードａを解放すると、次に、待ち状態となっているアプリ２が排他を獲得し、カードａに対してＰＩＮ認証を行った後内部のデータにアクセスする。この様に排他制御機構１１を設けることにより、認証を受けた１つのアプリケーションのみスマートカードに対してアクセスすることが出来、各アプリケーション２１毎の認証を実現することが出来る。

【００２０】

この図１の構成による方式の場合、１つのアプリケーション２１がスマートカード２２を使用している間このスマートカード２２はこのアプリケーション２１に専有されるので、他のアプリケーション２１は排他が解除されスマートカード２２が解放されるまで待ち状態になる。よってこの方式では、複数のアプリケーションの並列処理性能が悪く、また待ち状態にあるアプリケーションは長い期間処理を停止してハングアップした状態に見える等、非常に使い勝手が悪くなる。

【００２１】

これを回避するものとしては、アプリケーション２１がスマートカード２２へのアクセス処理が完了すると専有していたスマートカード２２を逐一解放する方式がある。この方式では、アプリケーション２１が複数回スマートカード２２に対するアクセス処理を含む場合、各アクセス処理毎に排他制御機構１１に対してスマートカード２２への排他獲得／解放を行い、こまめに排他制御を区切る。

【００２２】

図２に、この方式による各アプリケーションのスマートカードへの排他獲得／解放の例を示す。

同図は、図１と同様アプリ１、アプリ２及びアプリ３の３つのアプリケーショ

ン２１がカードａに対してアクセス要求を発行した場合の各アプリケーションのスマートカードへのアクセス処理例を示すもので、同図中排他制御機構１１への矢印↑は、各アプリケーション２１から排他制御機構１１への排他獲得要求、排他制御機構１１からの矢印↓は排他制御機構１１から各アプリケーション２１への排他獲得の通知を示す。また斜線部分は各アプリケーション２１によるＰＩＮ認証処理、網掛け部分はスマートカード２２へアクセス処理を示す。

【００２３】

排他を獲得したアプリケーション２１が、全処理が完了するまで排他を解除してスマートカード２２を解放しなかった場合、アプリ２は排他制御機構１１にカードａへの排他獲得要求を行った図２中の３１の位置から、既にカードａへの排他を獲得しているアプリ１が処理が完了する３３の位置まで、更にアプリ３は３２の位置からこのアプリ２の処理が完了するまで待ち状態となる。しかし、同図の様にアプリケーション２１が各アクセス処理毎にこまめに排他制御を区切ることにより、排他が解除された期間に別のアプリケーション２１がカードａにアクセスすることが出来るので、排他獲得の為の待ち状態となり処理が停止してしまう期間が短くなり、処理の並列性が向上する。

【００２４】

この様に、排他制御を頻繁に切替えると、各アプリケーションの待ち状態の期間は短くなり処理の並列性は向上する。しかし図２の斜線部に示すように各アプリケーションは切替えの度に認証状態の設定／解除処理を行う必要があり、その為のオーバヘッドが大きくなってしまう。また認証の再許可を得る際ＰＩＮを送信するので、各アプリケーション２１がＰＩＮを保持し続けることになり、セキュリティ上の問題も生じる。これを回避するため、認証処理の度にユーザがパスワードを入力する構成とすると更に認証処理のオーバヘッドが大きくなる。

【００２５】

図３にこの点を考慮した構成を示す。

図３の構成では、複数のアプリケーション２１とスマートカード２２の間に、排他制御機構１１に加えアクセス制御機構１２を設け、このアクセス制御機構１２によって各アプリケーション２１のスマートカード２２による認証を一元管理

しながら、排他制御機構１１がスマートカード２２にアクセスするアプリケーション２１の排他処理を行っている。

【００２６】

各アプリケーション２１はスマートカード２２に対してアクセスを要求する際、まず排他制御機構１１に対して排他獲得要求を行い、排他が獲得できると次にアクセス制御機構１２にスマートカード２２への認証を依頼する。そして認証が得られるとスマートカード２２内のデータにアクセスする。

【００２７】

アクセス制御機構１２は認証状態管理テーブルを持ち、この認証状態管理テーブルを用いてアプリケーション２１がスマートカード２２への認証の開始宣言を行ってから認証の解除を通知するまでの間について各アプリケーションとスマートカード２２との認証状態の管理を行う。

【００２８】

図４は、認証状態管理テーブルの構成例を示す図である。

認証状態管理テーブルは、各アプリケーション２１が現在どのスマートカード２２から認証を得ているのかを排他制御機構１１が管理するために用いるテーブルで、アプリ識別情報と認証済みカード情報を対応づけて記憶している。アプリ識別情報は、各アプリケーション２１を識別するための一意な識別子を記憶するもので、この識別子は、一般のアプリケーションが操作できないものが用いられ、例えばプロセス生成時に各プロセスに付加され、カーネルが管理しているプロセスＩＤを用いる。あるいは、スマートカードへアクセスへのアクセス要求を行ったアプリケーション２１に対してアクセス制御機構１２が識別子を順次生成付加してゆく構成としてもよい。

【００２９】

図４はカードａ，ｂの２つのスマートカード２２に対する各アプリケーション２１の認証状態を管理する場合を例示しており、各アプリケーションに対し認証済みカード情報としてそのアプリケーション２１が認証されているカードが記録されている。尚認証済みカード情報が空欄の部分は、そのアプリケーションに対し認証済みとなっているスマートカードが存在しないことを示す。同図では、ア

プリ１はカードａ，ｂ両方が認証済み、アプリ２、アプリｎはいずれも未認証、アプリ３はカードａのみ認証済みととなっている。

【００３０】

各アプリケーション２１は、スマートカード２２に対する認証及びスマートカード２２へのアクセスをアクセス制御機構１２を介して行う。アプリケーション２１からスマートカード２２へのアクセス要求が有ると、認証状態管理テーブルを参照してそのアプリケーション２１がアクセス要求したスマートカード２２に認証済みであるかどうかを調べ、未認証ならばアプリケーション２１からの要求を拒絶し、またアプリケーション２１にＰＩＮの入力を要求してスマートカード２２との認証処理を行う。また、そのアプリケーション２１が認証済みならばアプリケーション２１は既にそのスマートカード２１の認証許可を得ているのでスマートカード２１へのアクセスを許可し、実行する。

【００３１】

図５はアプリケーション２１がスマートカード２２へのアクセスを行う際の、アプリケーション２１、排他制御機構１１及びアクセス制御機構１２の処理の流れを示した図である。同図はアプリ１がカードａに対してアクセスを行う場合を例としており、また以下の説明中の１）～２３）は図５中の番号と対応している。

１）アプリ１はカードａへの排他開始を行うため、排他制御機構１１に対し、排他獲得要求を行う。

２）アプリ１からの要求に対し、排他制御機構１１は、カードａに対し排他獲得済のアプリケーションが有るか調べ、既に他のアプリケーションが獲得していたならば排他待ちのキューに登録する。また排他獲得済でなければ、アプリ１に排他獲得を通知する。

３）アプリ１は、アクセス制御機構１２にカードａへのアクセス開始宣言を行う。

４）アクセス開始宣言に対しアクセス制御機構１２は、認証状態管理テーブルにアプリ１を登録する。そして、アプリ１にＰＩＮの入力要求を行う。尚アプリ１がカードｂにもアクセス開始宣言を行っている場合は、アプリ１は既に認証状態

管理テーブルに登録してあるのでカードａに対するアクセス開始宣言で再度認証状態管理テーブルに登録する必要はない。

５）アプリ１はユーザにパスワードの入力を促し、ユーザの入力からＰＩＮを指定してカードａへの認証を要求する。

６）排他制御機構１１は、カードａに対しＰＩＮを通知し、カードａに認証チェックを行わせる。

７）アクセス制御機構１２は、カードａによる認証チェックの結果、認証が得られれば、認証状態管理テーブルにアプリ１がカードａに認証済みであることを登録する。

８）アプリ１はアクセス制御機構１２に対し、カードａへのデータの読み出し／書込みを要求する。

９）アプリ１からの読み出し／書込み要求に対し、認証状態管理テーブルを検索し、アプリ１が認証済カードａに認証済みならばカードａに対してアクセスを行う。未認証ならば、アプリ１にエラーを通知する。

１０）１つのアクセス処理が完了しカードａの専有を解除する場合に、アプリ１は排他制御機構１１に排他の解除を通知する。

１１）排他制御機構１１は、登録されているアプリ１のカードａに対する排他獲得を削除し、他にカードａへの排他待ちのキューに登録されているアプリケーション２１があればそのアプリケーション２１の排他獲得を登録する。

１２）排他の解除後、アプリ１はカードａへのアクセス処理以外の処理を行う。この間、カードａの排他を解放しているので他のアプリケーション２１がカードａを使用することが出来る。

１３）アプリ１は、再度カードａへのアクセスの必要が生じると、排他制御機構１１に排他獲得要求を行う。

１４）アプリ１からの要求に対し、排他制御機構１１は２）と同様、カードａに対し排他獲得済のアプリケーションが有るか再度調べ、既に他のアプリケーションが排他獲得済でなければ、アプリ１に排他獲得を通知する。

１５）アプリ１はアクセス制御機構１２に対し、カードａへのデータの読み出し／書込みを要求する。

１６）アクセス制御機構１２は、再度９）と同様な処理を行う。この時７）で、認証状態管理テーブルにアプリ１がカードａに認証済みであることが登録されているので、そのままカードａへアクセスを行う。以降アプリ１内のカードａへのアクセス処理の回数分１０）～１６）の処理が繰り返される。

１７）全アクセス処理が完了するとアプリ１は、アクセス制御機構１２にカードａへの認証を解除を通知する。

１８）アクセス制御機構１２は、認証状態管理テーブルのアプリ１からカードａ認証済の情報を削除する。

１９）アクセス制御機構１２は、認証状態管理テーブル１３に他にカードａに認証されているアプリケーション２１が存在しなくなるまで認証状態を保持し、認証されているアプリケーション２１存在しなくなるとカードａに認証解除を要求する。これにより同一のスマートカードとの認証処理の回数を削減することが出来る。

２０）アプリ１は、アクセス制御機構１２にスマートカード２２へのアクセス終了を通知する。

２１）２０）での通知を受けるとアクセス制御機構１２は認証状態管理テーブルから、アプリ１を削除する。この時アプリ１が他のスマートカード２２に対してはまだアクセスを終了していない場合は認証状態管理テーブルからアプリ１を削除しない。

２２）アプリ１は排他制御機構１１にカードａの排他の解除を通知する。

２３）排他制御機構１１は、再度１１）と同様な処理を行い、排他を解除する。

【００３２】

図６は、図３の排他制御機構１１及びアクセス制御機構１２を備えた構成による各アプリケーションへのスマートカードへの処理を示す図である。

同図は、比較のため図２と同じ前提の元での同じアプリケーション２１の処理を示してある。図６を図２比較すると、各アプリケーション２１は、認証処理としては、一番最初のカードａへのアクセス処理開始時のＰＩＮによる認証処理と、一番最後のアクセス処理終了時にカードａへの認証の解除処理を行っているのみで、図２では行っていたカードａへの各アクセス処理毎の認証処理が省略され

ている。よって各アプリケーション２１は認証処理が省略された分処理時間が短くなる。また各アプリケーション２１が、カードａを専有している期間も認証処理が省かれた分だけ短くなるので、その分待ち状態となる期間が短くてすむ可能性がある。更に各アプリケーション２１は、スマートカード２２に対するＰＩＮ認証を最初に１度だけ行えばよいので、カードから認証が得られればＰＩＮを破棄することが出来る。

【００３３】

図７は、本システムによりスマートカード２２にアクセスを行うアプリケーション２１の処理を示すフローチャートである。

尚これらの処理を行う機構をアプリケーション２１に直接持たせる構成とすることも出来るが、これらの処理をライブラリとして実現し、このライブラリを各アプリケーション２１に組込む形態を取るのが一般的な構成である。

【００３４】

アプリケーション２１は、スマートカード２２にアクセスを行う際、まず排他制御機構１１へ排他獲得の依頼を行い（ステップＳ１）、排他制御機構１１からの応答を待つ。その結果、排他制御機構１１から何等かの理由で、排他が獲得出来ない旨の通知が有れば（ステップＳ２、ＮＯ）、処理を終了する。

【００３５】

排他獲得の依頼に対し、排他制御機構１１から排他獲得成功の通知が有れば（ステップＳ２、ＹＥＳ）、次にステップＳ３として、アクセス制御機構１２にスマートカード２２へのアクセスの開始宣言を行う。

【００３６】

このスマートカード２２へのアクセスが未認証のスマートカード２２へのアクセスであり、スマートカード２２への認証が必要なためアクセス制御機構１２からＰＩＮの入力を要求された時（ステップＳ４、ＹＥＳ）、ステップＳ８としてアクセス制御機構１２にＰＩＮとしてユーザが入力したパスワードをアクセス制御機構１２に送って、認証処理を依頼し確認を行う。その結果認証されれば（ステップＳ９、ＹＥＳ）、処理をステップＳ５に移してスマートカードへアクセスし、認証されなければ（ステップＳ９、ＮＯ）、処理を終了する。

【００３７】

ステップＳ４において、このアクセスが既に認証を得ているスマートカード２２へのアクセスである時（ステップＳ４、ＮＯ）、更なる認証処理は必要無いので、ステップＳ５としてスマートカード２２へのアクセスを許可してデータの読み出し／書込みを行う。

【００３８】

ステップＳ５のアクセス処理が終了すると、ステップＳ６として、アクセス制御機構１２に対してスマートカード２２へのアクセスの終了宣言を行う。そしてステップＳ７として、そのスマートカード２２への排他の解除を排他制御機構１１に通知して処理をスマートカード２２へのアクセス処理を終了する。

【００３９】

図８は、アプリケーション２１からの排他獲得要求に対する排他制御機構１１の処理を示すフローチャートである。

アプリケーション２１から、スマートカード２２への排他獲得要求があると、排他制御機構１１は、ステップＳ１１として、排他獲得を要求されたスマートカード２２が、既に他のアプリケーション２１によって排他獲得済みであるかどうかが判断される。その結果他のアプリケーション２１による排他獲得が行われていなければ（ステップＳ１１、ＮＯ）、そのスマートカード２２を排他獲得済みとして登録し、要求を行ったアプリケーション２２に排他獲得を通知して処理を終了する。

【００４０】

またステップＳ１１で他のアプリケーション２１が排他獲得済みであるならば（ステップＳ１１、ＹＥＳ）、ステップＳ１２としてこの排他獲得要求を排他待ちキューに追加して処理を終了する。

【００４１】

図９は、アプリケーション２１からの排他の解除通知に対する排他制御機構１１の処理を示すフローチャートである。

アプリケーション２１からスマートカード２２への排他の解除通知を受けると、排他制御機構１１は、ステップＳ２１としてそのアプリケーション２２の排他

獲得済みの登録を削除して排他を解除する。

【００４２】

そして排他待ちキューを調べ、排他が解除されたスマートカード２２に対して排他待ちとなっているアプリケーション２１が存在すれば（ステップＳ２２、ＹＥＳ）、排他待ちキューの先頭に登録されているアプリケーション２１のそのスマートカード２２への排他獲得を登録してスマートカード２２をディスパッチした後、また排他待ちキューに待ちが存在しなければ（ステップＳ２２、ＮＯ）そのまま、処理を終了する。

【００４３】

図１０は、アプリケーション２１からのスマートカード２２へのアクセス要求に対するアクセス制御機構１２の処理を示すフローチャートである。

アプリケーション２１からのアクセス開始宣言に対し、アクセス制御機構１２は、ステップＳ３１として、認証状態管理テーブルにアプリ１を登録して、スマートカード２２に対してアクセス要求プロセスを登録する。

【００４４】

図１１は、アプリケーション２１からのスマートカード２２へのアクセス要求に対するアクセス制御機構１２の処理を示すフローチャートである。

アプリケーション２１からのアクセス要求に対し、アクセス制御機構１２はステップＳ４１として認証状態管理テーブルを参照して、そのアプリケーション２１がアクセス要求先のスマートカード２２から既に認証済であるかどうか調べる。その結果、既に認証済みであれば（ステップＳ４１、ＹＥＳ）、更なる認証は必要無いので、ステップＳ４５としてアプリケーション２１に対してアクセス許可を通知する。

【００４５】

ステップＳ４１で、そのアプリケーション２１がまだ認証を得ていないのならば（ステップＳ４１、ＮＯ）、認証処理を行う必要があるので、ステップＳ４２としてアプリケーション２１にパスワードの入力を要求し、スマートカード２２に対してＰＩＮによる認証チェックを依頼する。その結果、スマートカード２２から認証が得られれば、ステップＳ４５としてアプリケーション２１に対してア

クセス許可を通知し、また認証が得られなければ（ステップＳ４３、ＮＯ）、アクセス不許可をアプリケーション２１に対して通知して処理を終了する。

【００４６】

図１２は、本実施形態に於けるスマートカードを使用するシステムの構成を示す図である。

本実施形態でのアプリケーション４１とスマートカード４２との間を管理するアクセス管理システム４０は、スマートカードリーダ４１と各アプリケーション４１のライブラリ４４との間に構成され、ＯＳの一機能として、あるいはＯＳに実装される形で実現される。

【００４７】

アプリケーション４１は、スマートカード４２に対する認証処理やアクセス処理を、全てこのアクセス制御システム４０を介して行い、アクセス制御システム４０は、各アプリケーション４１とスマートカード４２との間のやり取りを把握している。またアクセス制御システム４０は、スマートカードリーダ４３の状態も把握しており、例えばスマートカードリーダ４３からスマートカード４２が抜かれると、認証状態管理テーブルを調べ、そのカードが認証済みとしているアプリケーションがあれば未認証に変更する。

【００４８】

なお、アクセス管理システム４０は、内部に排他制御機構１１とアクセス制御機構１２を別々に持つ構成となっているが、これらを１つの機能構成要素として実現することもできる。また、セキュリティ上、アクセス制御機構や排他制御機構は、複数のアプリケーションが共有できる必要があるので、ＯＳのカーネル内に実現するとセキュリティをより向上することができる。

【００４９】

図１３は、本実施形態における上記スマートカードのアクセス管理をコンピュータプログラムにより実現した場合の情報処理装置のシステム環境図である。

スマートカードを実装した情報処理装置は、図１３の様にＣＰＵ５１、ＲＯＭ、ＲＡＭによる主記憶装置５２、補助記憶装置５３、ディスプレイ、キーボード等の入出力装置（Ｉ／Ｏ）５４、ＬＡＮやＷＡＮ、一般回線等により他ノードと

ネットワーク接続を行うモデム等のネットワーク接続装置５５、ディスク、磁気テープなどの可搬記録媒体５７から記憶内容を読み出す媒体読取り装置５６及び１乃至複数のいスマートカード５９を実装しているスマートカードリーダ５８を有し、これらが互いにバス６０により接続される構成を備えている。

【００５０】

また図１３の情報処理システムでは、媒体読取り装置５６により磁気テープ、フロッピーディスク、ＣＤ－ＲＯＭ、ＭＯ等の記録媒体５７に記憶されているプログラム、データを読み出し、これを主記憶装置５２またはハードディスク５５にダウンロードする。そして本実施形態による各処理は、ＣＰＵ５１がこのプログラムやデータを実行することにより、ソフトウエア的に実現することが可能である。

【００５１】

また、この情報処理装置では、フロッピーディスク等の記録媒体５７を用いてアプリケーションソフトの交換が行われる場合がある。よって、本発明は、計測制御用監視端末やその画面の操作方法に限らず、コンピュータにより使用されたときに、上述の本発明の実施の形態の機能をコンピュータに行わせるためのコンピュータ読み出し可能な記録媒体５７として構成することもできる。

【００５２】

この場合、「記録媒体」には、例えば図１４に示されるように、ＣＤ－ＲＯＭ、フロッピーディスク（あるいはＭＯ、ＤＶＤ、リムーバブルハードディスク等であってもよい）等の媒体駆動装置７７に脱着可能な可搬記録媒体７６や、ネットワーク回線７３経由で送信される外部の装置（サーバ等）内の記憶手段（データベース等）７２、あるいは情報処理装置７１の本体７４内のメモリ（ＲＡＭ又はハードディスク等）７５等が含まれる。可搬記録媒体７６や記憶手段（データベース等）７２に記憶されているプログラムは、本体７４内のメモリ（ＲＡＭ又はハードディスク等）７５にロードされて、実行される。

【００５３】

（付記１）　複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードのアクセス管理システムであって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする排他制御手段と、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可するアクセス制御手段と

を備えることを特徴とするアクセス管理システム。

【００５４】

（付記２）　前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録することを特徴とする付記１に記載のアクセス管理システム。

【００５５】

（付記３）　前記アクセス制御手段は、前記アクセス要求に対し、前記排他を獲得したアプリケーションが前記スマートカードから未認証である時、該アプリケーションの要求を拒絶することを特徴とする付記１又は２に記載のアクセス管理システム。

【００５６】

（付記４）　前記アクセス制御手段は、アプリケーションとスマートカードとの認証関係を該アプリケーションのプロセスＩＤを用いて管理することを特徴とする付記１乃至３のいずれか１に記載のアクセス管理システム。

【００５７】

（付記５）　前記アクセス制御手段は、前記スマートカードがスマートカードリーダより抜かれた時、該抜かれたスマートカードにより認証済みとなっているアプリケーションを未認証に変更することを特徴とする付記１乃至４のいずれか１に記載のアクセス管理システム。

【００５８】

（付記６）　前記アプリケーションは、前記スマートカードに複数回アクセスする時、各アクセスの開始時に前記排他制御手段に前記排他獲得要求を行い、該各アクセスの終了時に前記排他制御手段に排他の解除通知を行うことを特徴とする付記１乃至５のいずれか１に記載のアクセス管理システム。

【００５９】

（付記７）　前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードが他のアプリケーションによって既に排他獲得済みであれば、該排他獲得要求を行ったアプリケーションをキューに登録し、前記アプリケーションからの排他の解除通知に対し、前記キューに登録されているアプリケーションを排他獲得済みとすることを特徴とする付記６に記載のアクセス管理システム。

【００６０】

（付記８）　前記アクセス制御手段は、アプリケーションからスマートカードの認証解除の通知に対し、該認証解除が該スマートカードにより認証済みとなっている最後のアプリケーションからの時、該スマートカードに認証解除を要求することを特徴とする付記１乃至７のいずれか１に記載のアクセス管理システム。

【００６１】

（付記９）　複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードの共有方法であって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを特徴とする共有方法。

【００６２】

（付記１０）　１つのスマートカードへの複数のアクセス処理を含むアプリケ

ーション又はそのライブラリであって、

前記各アクセス処理に対し、該アクセス処理の開始時にそれぞれ前記排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、

前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーション又はそのライブラリ。

【００６３】

（付記１１）　１つスマートカードへの複数のアクセス処理を含むアプリケーションのライブラリであって、

前記各アクセス処理に対し、該アクセス処理の開始時にそれぞれ前記排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、

前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーションのライブラリ。

【００６４】

（付記１２）　複数のアプリケーションが並列動作する情報処理装置によって使用された時、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを前記情報処理装置に行わせるプログラムを記憶した前記情報処理装置が読み出し可能な記録媒体。

【００６５】

【発明の効果】

本発明によれば、排他制御によりスマートカードに対する排他制御が行われるので、複数のアプリケーションによってスマートカードを共用しても各アプリケ

ーション単位の認証を可能とする。

【００６６】

また、各アプリケーションとスマートカードとの間の認証関係が一元管理されているので、アプリケーションがスマートカードにアクセス要求を行うとそのスマートカードはそのアプリケーションを認証済みかどうかが判断され、未認証の場合のみ認証処理が行われるので、認証処理回数を削減することが出来、認証処理によるオーバヘッドを小さくすることが出来る。またＰＩＮによる認証処理は、最初に一度だけ行われるのでアプリケーションは、ＰＩＮを保持し続ける必要がなく、セキュリティレベルの向上が図れる。

【００６７】

更にスマートカードは、認証状態を保持したまま複数の認証済みアプリケーションとの間でアクセスが可能となる。

またアプリケーションは、排他獲得の為の待ち状態期間を短く出来る。よって処理の並列性を向上出来また各アプリケーションの処理時間の短縮を図れる。

【図面の簡単な説明】

【図１】

排他制御機構を設け、スマートカードへのアクセスの排他処理を行った場合の構成を示す図である。

【図２】

排他制御機構を備えた構成時の各アプリケーションへのスマートカードへのアクセス処理を示す図である。

【図３】

排他制御機構及びアクセス制御機構を設けた場合の構成図である。

【図４】

認証状態管理テーブルの構成例を示す図である。

【図５】

アプリケーションがスマートカードへのアクセスを行う際の、アプリケーション、排他制御機構及びアクセス制御機構の処理の流れを示した図である。

【図６】

排他制御機構及びアクセス制御機構を備えた構成時の各アプリケーションへのスマートカードへのアクセス処理を示す図である。

【図７】

スマートカードにアクセスを行うアプリケーションの処理を示すフローチャートである。

【図８】

アプリケーションからの排他獲得要求に対する排他制御機構の処理を示すフローチャートである。

【図９】

アプリケーションからの排他の解除通知に対する排他制御機構の処理を示すフローチャートである。

【図１０】

アプリケーションからのスマートカードへのアクセス開始宣言に対するアクセス制御機構の処理を示すフローチャートである。

【図１１】

アプリケーションからのスマートカードへのアクセス要求に対するアクセス制御機構の処理を示すフローチャートである。

【図１２】

本実施形態に於けるスマートカードを使用するシステムの構成を示す図である。

【図１３】

情報処理装置のシステム環境図である。

【図１４】

記憶媒体の例を示す図である。

【図１５】

スマートカード内部の論理的構成を示す図である。

【符号の説明】

１１　排他制御機構

１２　アクセス制御機構

２１、４１　アプリケーション

２２、４２、５９　スマートカード

４０　アクセス制御システム

４３、５８　スマートカードリーダ

５１　ＣＰＵ

５２　主記憶装置

５５　補助記憶装置

５４　入出力装置

５５　ネットワーク接続装置

５６　媒体読取り装置

５７　可搬記憶媒体

６０　バス

７１　情報処理装置

７２　記憶手段

７３　ネットワーク回線

７４　情報処理装置本体（コンピュータ）

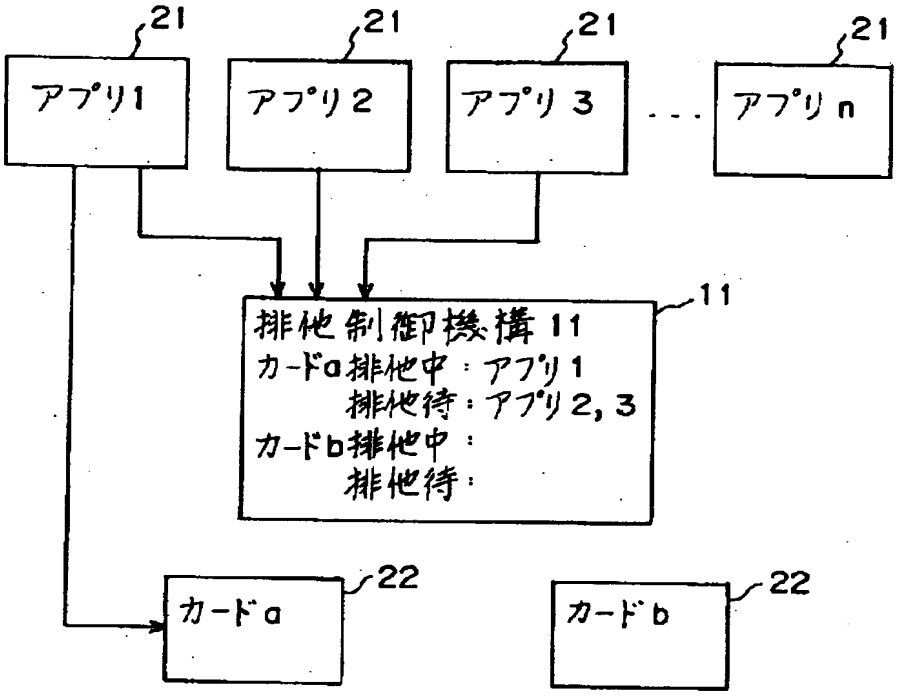
７５　メモリ

７６　可搬記録媒体

【書類名】　図面

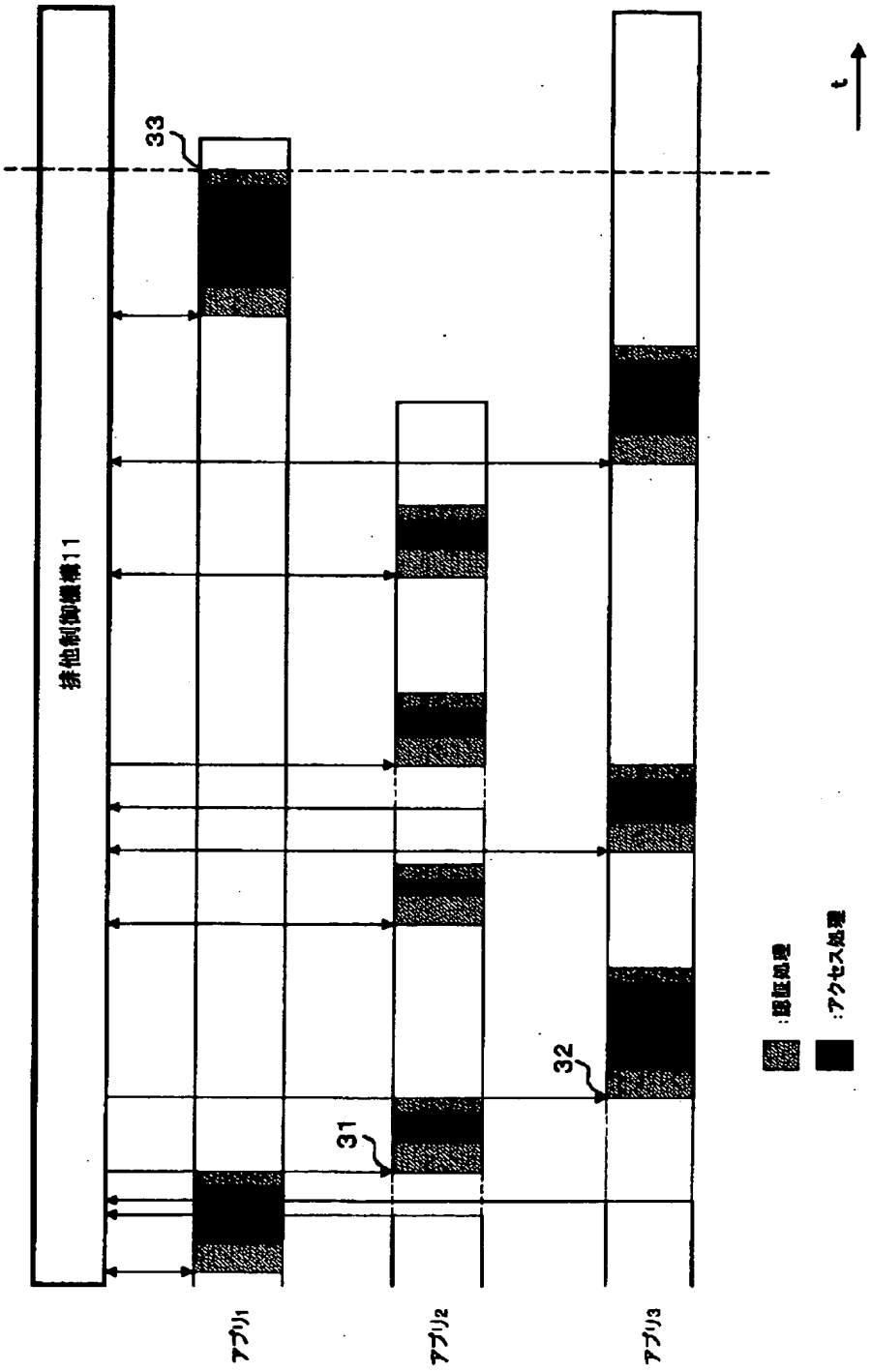
【図１】

排他制御機構を設け、スマートカードへのアクセスの排他処理を行った場合の構成を示す図



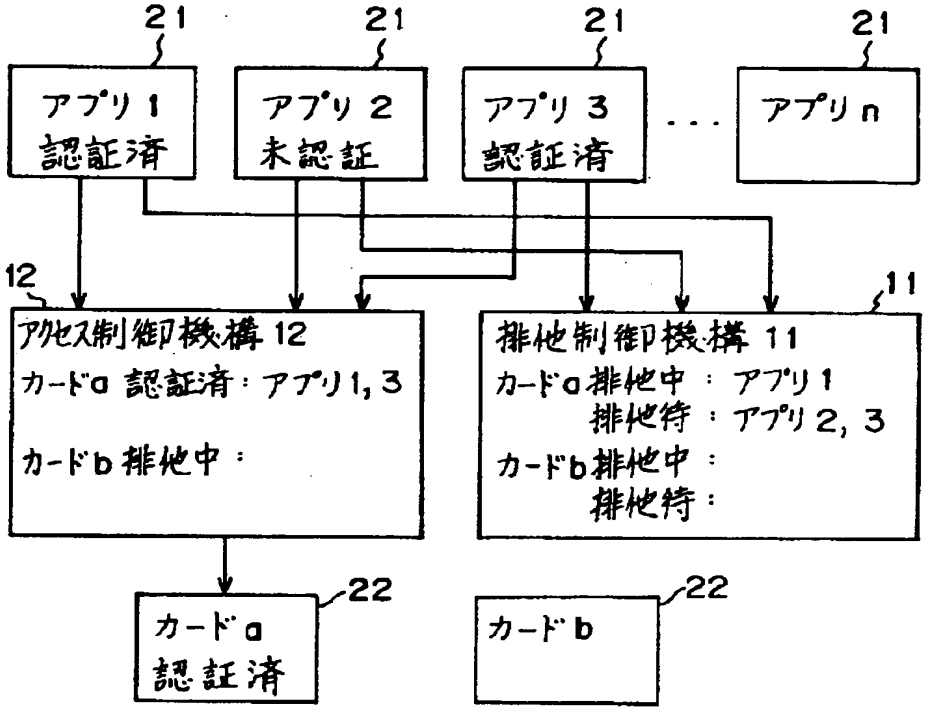
【図２】

排他制御機構を備えた構成時の各アプリケーションへのスマートカードへのアクセス処理を示す図



【図３】

排他制御機構及びアクセス制御機構を設けた場合の構成図



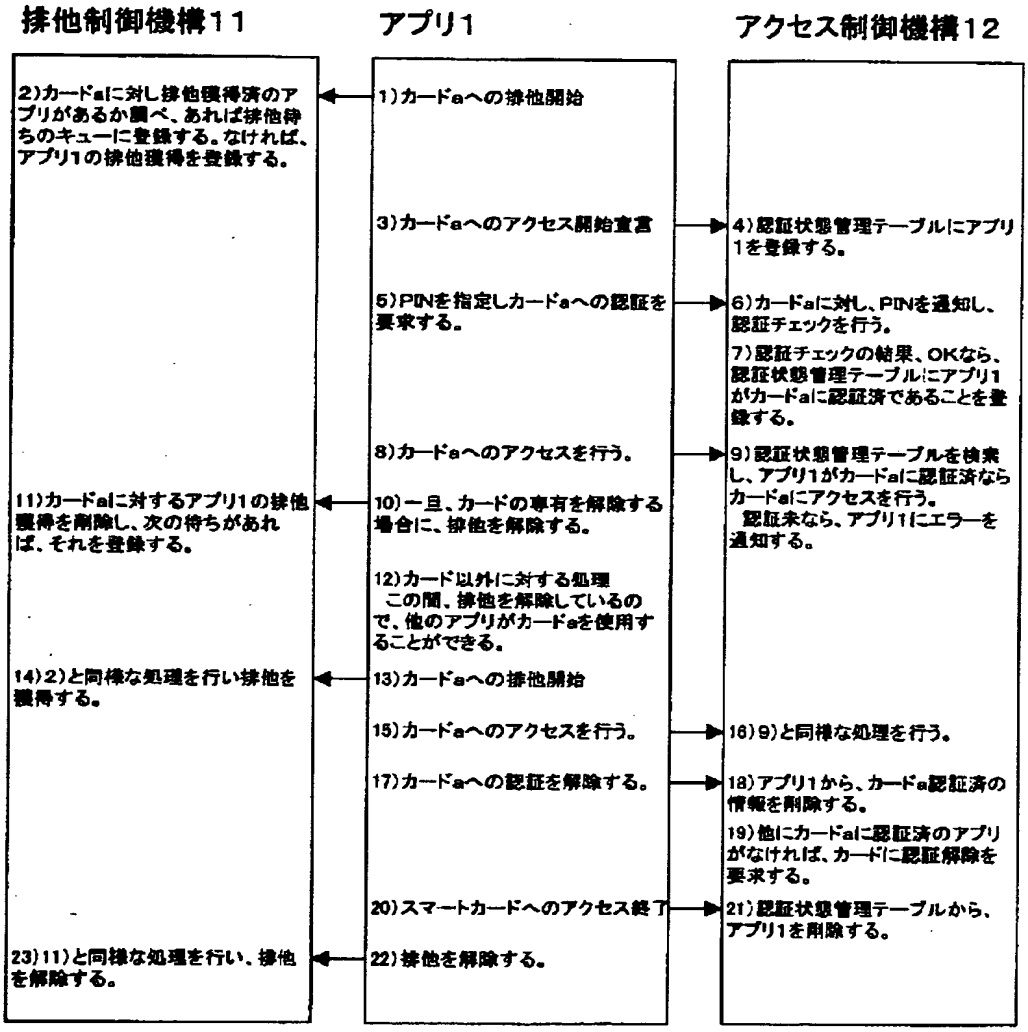
【図４】

認証状態管理テーブルの構成例を示す図

アプリ識別情報	認証済みカード情報	
アプリ1	カードa	カードb
アプリ2		
アプリ3	カードa	
……	……	……
アプリn		

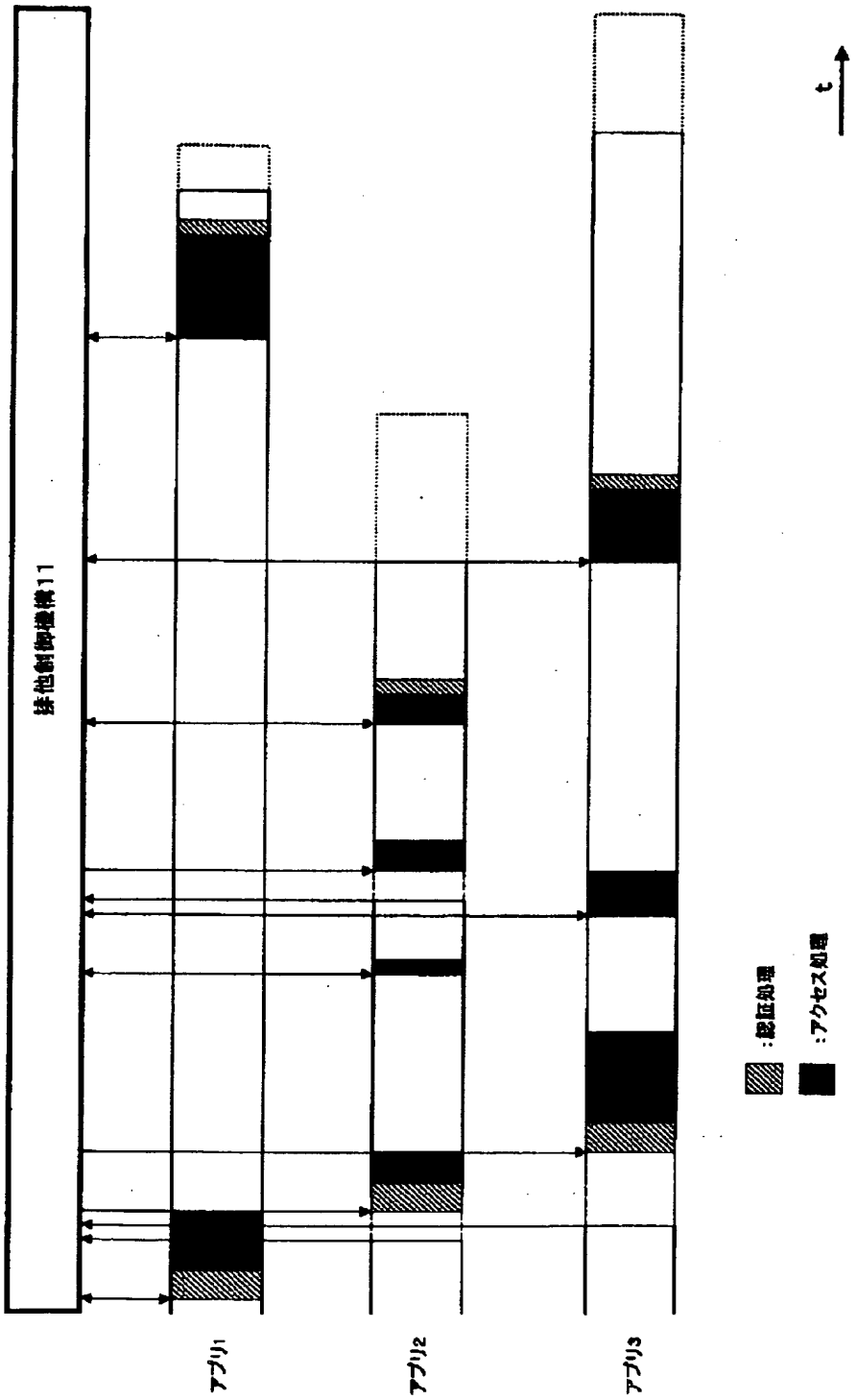
【図５】

アプリケーションがスマートカードへのアクセスを行う際の、アプリケーション、排他制御機構及びアクセス制御機構の処理の流れを示した図



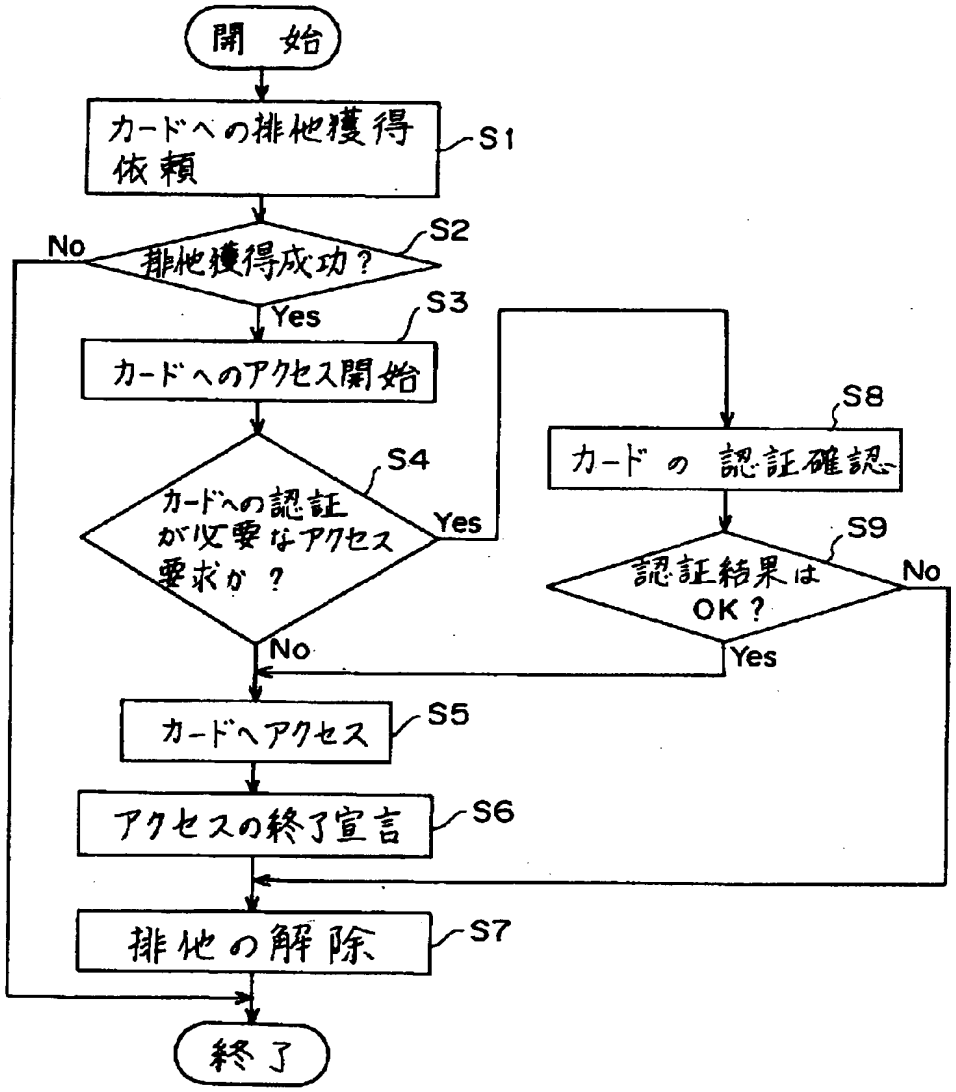
【図６】

排他制御機構及びアクセス制御機構を備えた構成時の
各アプリケーションへのスマートカードへのアクセス処理を示す図



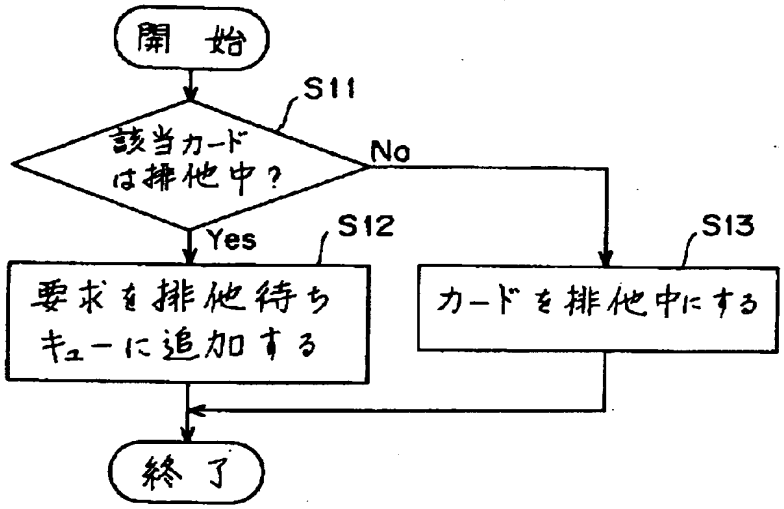
【図７】

スマートカードにアクセスを行うアプリケーションの処理を示すフローチャート



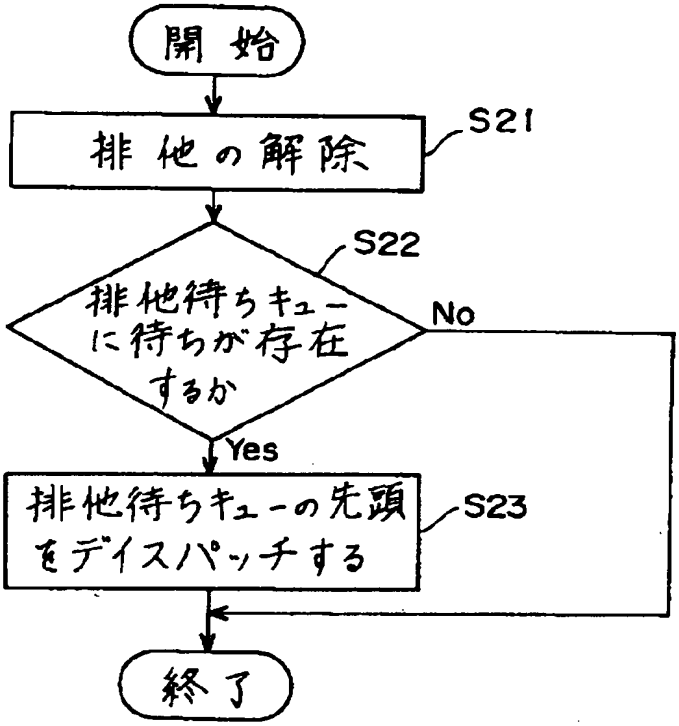
【図８】

アプリケーションからの排他獲得要求に対する
排他制御機構の処理を示すフローチャート



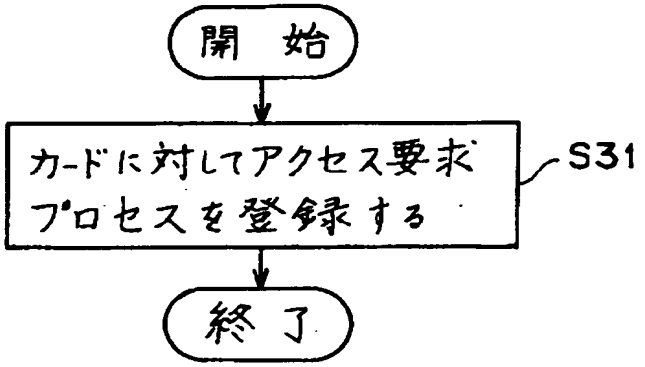
【図９】

アプリケーションからの排他の解除通知に対する排他制御機構の処理を示すフローチャート



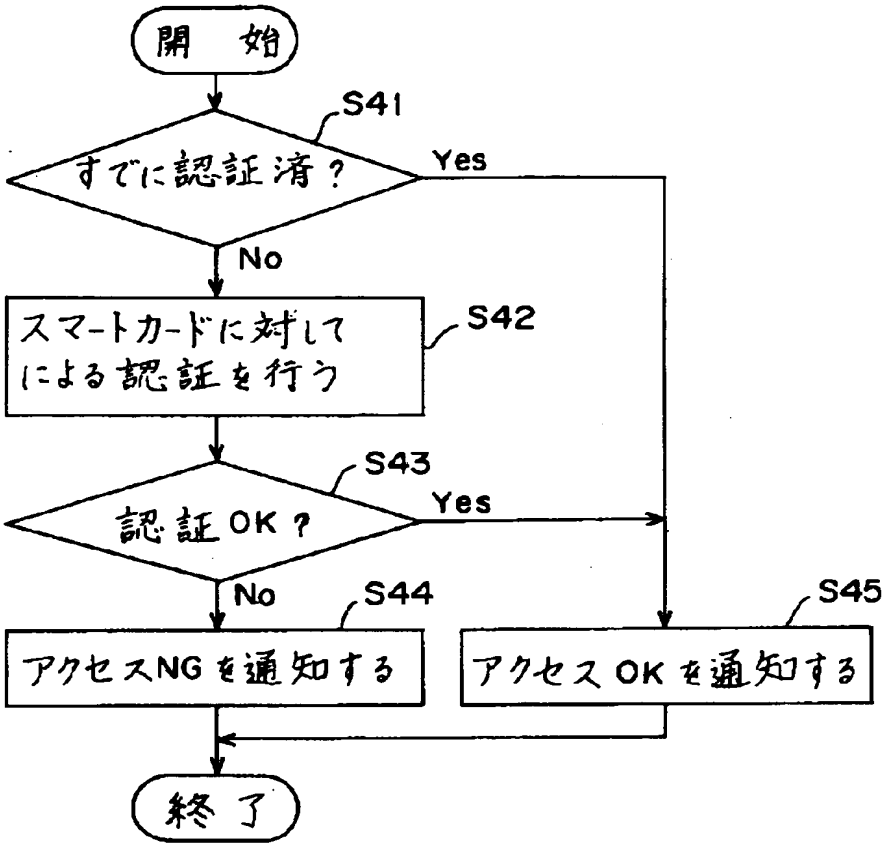
【図１０】

アプリケーションからのスマートカードへのアクセス開始宣言に対するアクセス制御機構の処理を示すフローチャート



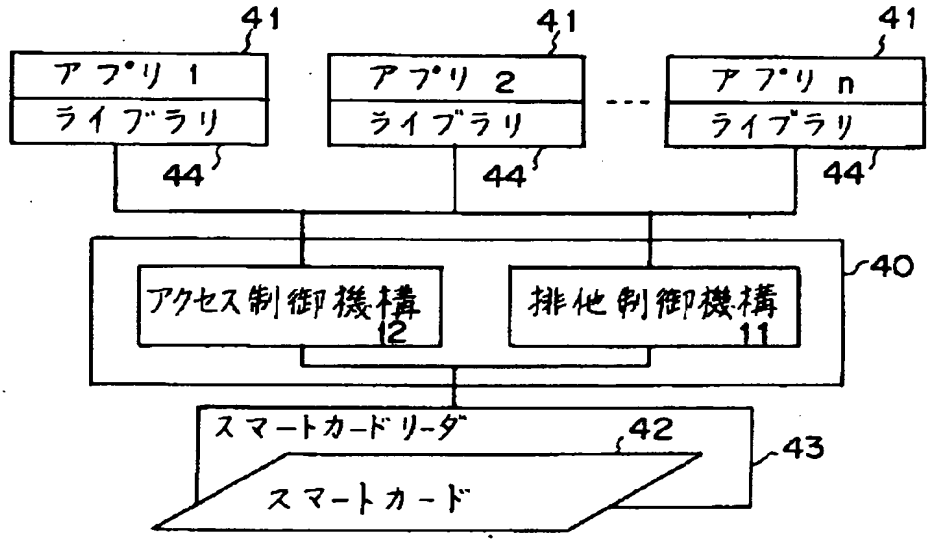
【図１１】

アプリケーションからのスマートカードへのアクセス要求に対するアクセス制御機構の処理を示すフローチャート



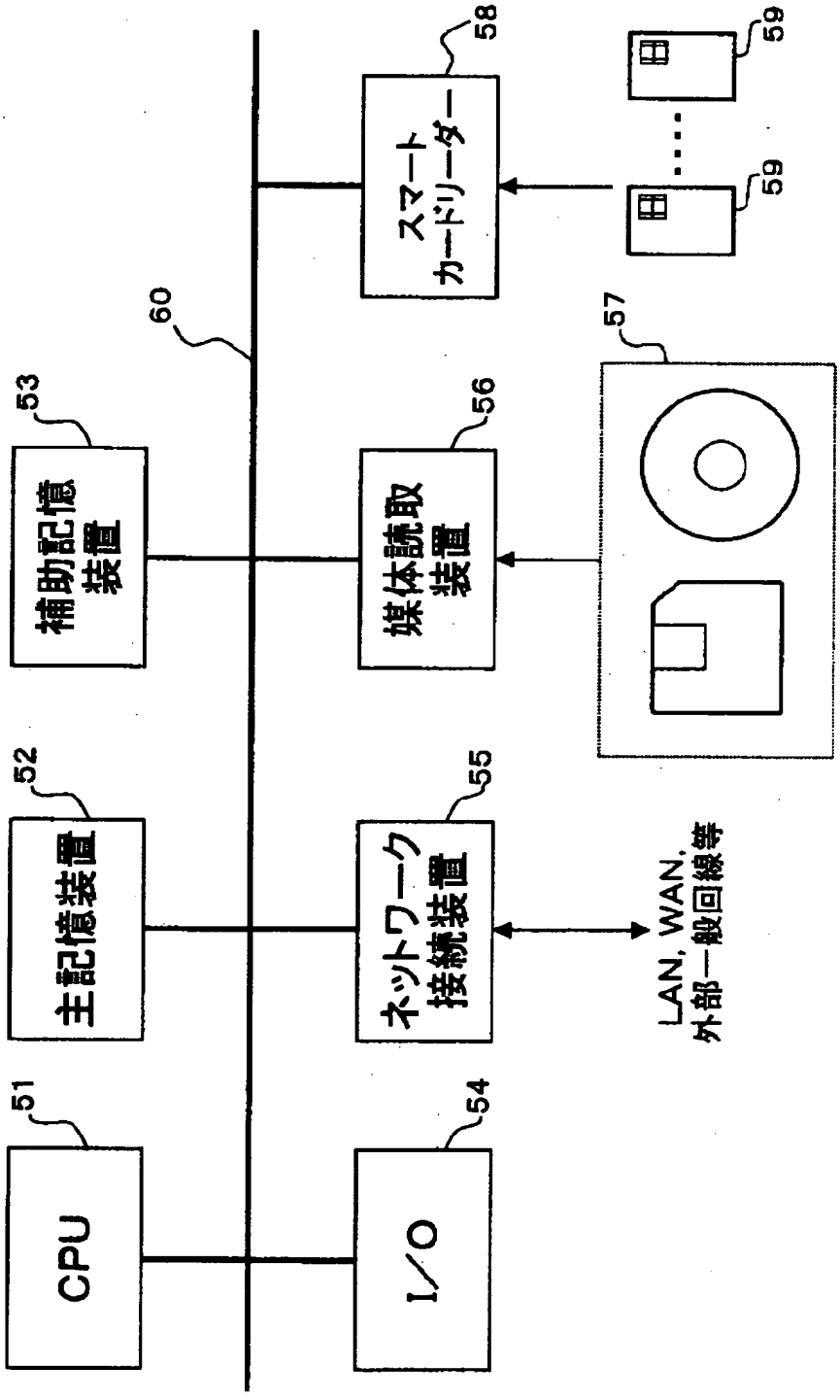
【図１２】

本実施形態に於けるスマートカードを使用するシステムの構成を示す図



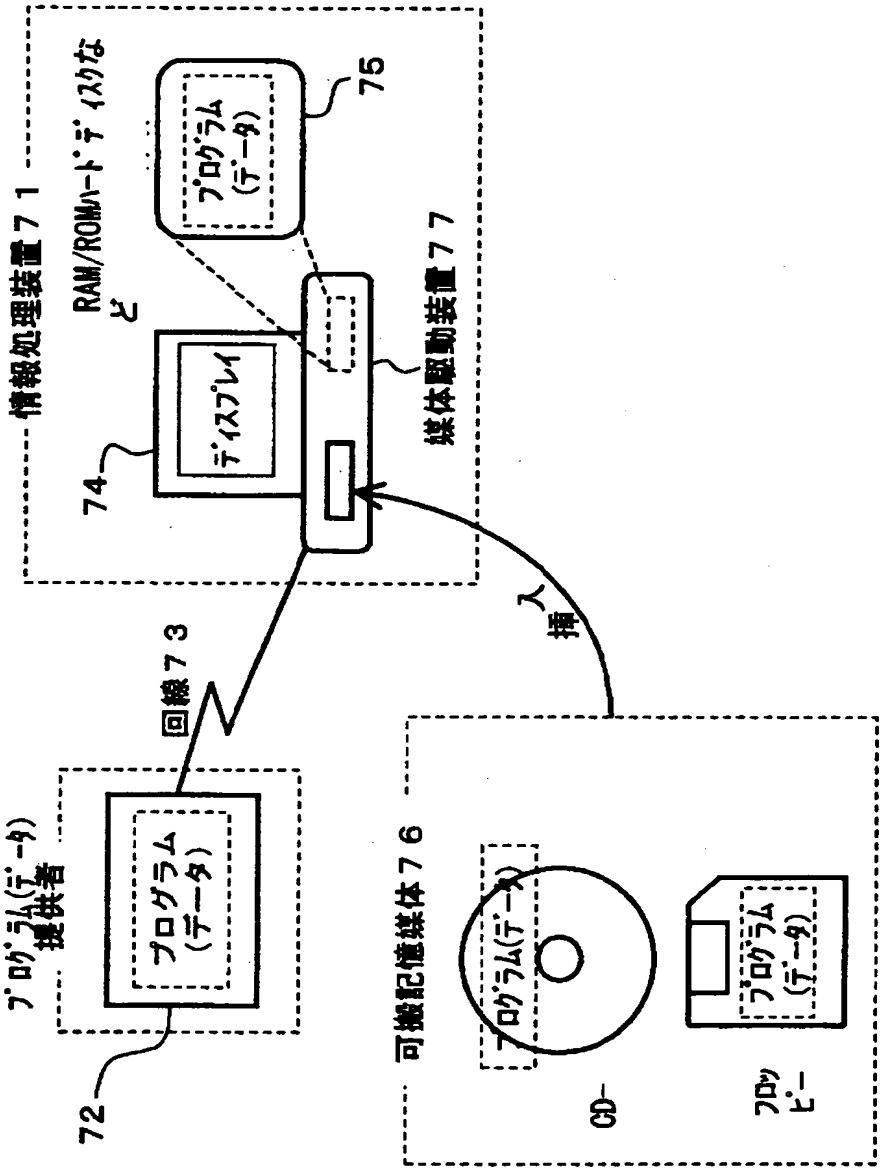
【図１３】

情報処理のシステム環境図



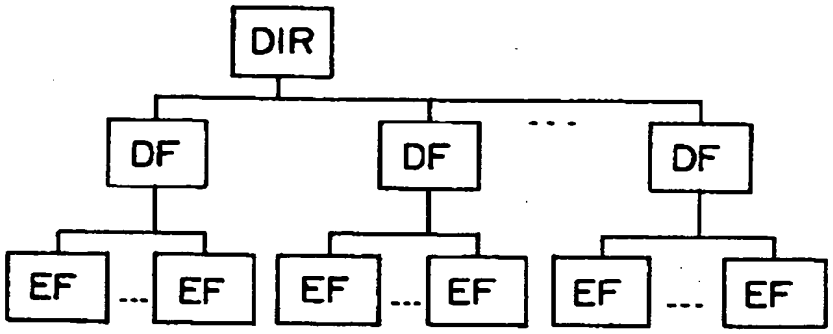
【図１４】

記憶媒体の例を示す図



【図１５】

スマートカード内部の論理的構成を示す図



【書類名】　　要約書

【要約】

【課題】　複数のアプリケーションによるアクセスに対し、各アプリケーション（プロセス）毎に認証許可を与えるスマートカードのアクセス管理システム及び管理方法を提供することを課題とする。

【解決手段】　スマートカードへの複数のアクセス処理を含むアプリケーション２１は、各アクセス処理毎にスマートカード２２に対してアクセス要求を行う際、排他制御機構１１に対して排他獲得要求を行い、排他が得られるとアクセス制御機構１２に対してアクセスを要求する。アクセス制御機構１２はアプリケーション２１が未認証ならばＰＩＮの入力を要求し、既に認証を得られていればスマートカード２２へのアクセスを許可する。アプリケーション２１はアクセス処理単位で排他獲得要求／解除を行う。

【選択図】　　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社